dishNET Wireline L.L.C.
9601 S. Meridian Blvd.
Englewood, CO 80112

March 1, 2016

VIA ELECTRONIC FILING

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th St., SW
Washington, DC 20554

RE: Annual CPNI Certification, EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's rules, 47 C.F.R. 64.2009(e), dishNET Wireline L.L.C. files its annual certification of compliance with the Commission's customer proprietary network information (CPNI) rules.

Sincerely,

_____/s/_____
Shawn Stickle
Vice President, Operations

Direct Dial: **303.723.1953** | Email: **Shawn.Stickle@dish.com**

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2016 covering the prior calendar year 2015

1. Date filed: March 1, 2016

2. Name of company covered by this certification: **dishNET Wireline, L.L.C**.

3. Form 499 Filer ID: 824050

4. Name of signatory: Shawn Stickle

5. Title of signatory: Vice President, Operations

6. Certification:

I, Shawn Stickle, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken any actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The Company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The Company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed: _____

Date: 3/1/2016

Attachment: Statement Concerning the Protection of Customer Proprietary Network Information

Statement Concerning the Protection of Customer Proprietary Network Information

1. dishNET Wireline L.L.C. is a telecommunications carrier subject to the requirements set forth in Section 64.2009 of the Federal Communications Commission's ("FCC's") rules. The Company has policies and procedures applicable to the FCC's rules pertaining to the use, disclosure and access to customer proprietary network information ("CPNI") set forth in sections 64.201 et. seq.

2. The Company has designated a CPNI Compliance Officer who is responsible for, to the extent applicable: (1) communicating with the Company's attorneys regarding CPNI responsibilities, requirements and restrictions; (2) supervising the training of Company employees and/or agents who use or have access to CPNI; (3) supervising the use, disclosure, distribution or access to the Company's CPNI by agents, independent contractors or joint venture partners; (4) maintaining records regarding the use of CPNI in marketing campaigns; and (5) receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.

3. Training provides Company personnel, agents, and contractors (as applicable) with information as to when they are and are not authorized to release or use CPNI, and violation of these policies will subject personnel to disciplinary action.

4. If a customer calls the Company requesting information that is considered CPNI, the Company will not release such information unless the customer is able to verify he or she is the authorized party on the account through provision of a password. If the customer cannot supply the password, the customer may be asked a series of challenge and answer questions, or may request that the information be sent to the customer's address of record.

5. The Company will not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

6. If and when customer approval to use, disclose, or permit access to customer CPNI is desired, the Company will obtain such customer approval. The Company honors a customer's approval or disapproval until the customer revokes or limits such approval or disapproval.

7. In the event the Company seeks to use CPNI information for any sales and marketing campaigns, supervisory approval will be required for any Company sales personnel's proposed outbound marketing request for customer approval of the use of CPNI and the Company will maintain records reflecting carrier compliance with the relevant Commission rules if applicable.

8. Prior to any solicitation for customer approval, the Company will provide notification to customers of their right to restrict use of, or disclosure of, and access to the

customer's CPNI. Records of these notifications will be maintained for a period of at least one year.

9. Any customer request to deny access to CPNI will not affect the provision of any services to which the customer subscribes.

10. The Company will maintain a record of its sales and marketing campaigns that use customer's CPNI, if the Company engages in such campaigns. Further, a record of instances where CPNI was disclosed or provided to third parties or where third parties were allowed access to CPNI will be maintained by the Company. These records will reflect a description of the campaigns, the specific CPNI used in the campaign and what products or services were offered as part of the campaign. These records will be retained for a minimum of one year.

11. Company will maintain appropriate records through which a customer's CPNI use opt-out status (if any) can be clearly established prior to the use of CPNI.

12. If a breach of CPNI occurs, the Company will provide electronic notification of the breach to the U.S. Secret Service ("USSS") and the FBI as soon as practicable and in no event more than seven (7) days after reasonable determination of the breach. The Company will also notify impacted customer(s) only after seven (7) more days have passed after notification to the USSS and the FBI, unless there is a risk of immediate and irreparable harm to the customer in which case the Company will notify the customer immediately after consulting with and in cooperation with the relevant investigative agency. Company will keep records or discovered breaches for at least two (2) years.